

United States Senate

WASHINGTON, DC 20510

January 18, 2019

Paul J. Wiedefeld
General Manager and CEO
Washington Metropolitan Area Transit Authority
600 5th Street, NW
Washington, DC 20001

Dear Mr. Wiedefeld:

As representatives of the National Capital Region, we write to raise concerns regarding the safety and security of the transportation network operated by the Washington Metropolitan Area Transit Authority (WMATA), particularly in regards to the procurement process that WMATA is currently undertaking to acquire new rail cars.

In the transportation sector, there has been increased interest from particular foreign governments to participate in state and local procurements, including those to manufacture and assemble rail cars for transit agencies around the country. While other cities have welcomed this kind of investment, we have serious concerns about similar activity happening here in our nation's capital, particularly when it could involve foreign governments that have explicitly sought to undermine our country's economic competitiveness and national security.

As Metro continues its procurement process for the 8000-series rail car, we strongly urge you to take the necessary steps to mitigate growing cyber risks to these cars. WMATA's Request for Proposals (RFP) issued in September 2018 lists the following technologies, among others, that may be incorporated into these trains: automatic train control; network and trainline control; video surveillance; monitoring and diagnostics; and data interface with WMATA, among others. Many of these technologies could be entirely susceptible to hacking, or other forms of interference, if adequate protections are not in place to ensure they are sourced from safe and reliable suppliers. In a Q&A document posted as part of the RFP, WMATA noted that there are "no Buy America or Disadvantaged Business Enterprise (DBE) requirements for this contract," raising further questions about what protections will be in place to ensure the integrity of these components.

Therefore, we ask that you please provide answers to the following questions as you continue the bidding process:

1. While we are aware that nearly all passenger railcar manufacturers in the United States are foreign-owned, what steps is WMATA taking to ascertain and mitigate against the involvement of foreign governments in this procurement?
2. Has Metro received briefings from the Department of Homeland Security or related agencies on the attempts of foreign adversaries to infiltrate our critical infrastructure and the significant cyber vulnerabilities that can stem from them doing so?
3. Will Metro take a company's ties to foreign governments with a record of industrial and cyber espionage into account when evaluating bids, particularly if such company is a state-owned enterprise?

4. If so, will Metro allow sensitive component parts of these railcars to be sourced from such countries?
5. Will Metro consult with the Department of Defense prior to awarding a contract to confirm whether the Department would permit railcars built by certain foreign governments to operate through the Pentagon?
6. We understand that Metro has announced that the RFP will be amended to include baseline cybersecurity protocols. Please provide information about these protocols and how they are being developed. How will Metro evaluate bidder responses to this forthcoming cybersecurity addendum? Will Metro review these responses with the Department of Transportation and the Department of Homeland Security, and seek the concurrence of USDOT and DHS in its cybersecurity evaluations before making any final contract award in this procurement? What specific requirements will the addendum include to ensure that any communications technology included in the rail car procurement is protected from being exploited for surveillance purposes?

We have raised the issue of prioritizing cybersecurity measures in the past, and in a Feb. 9, 2017 letter, you noted that "WMATA follows the industry best practices and frameworks...to effectively protect WMATA" from cyberattacks. We urge that you prioritize adopting robust cybersecurity protections, going beyond industry best practices if necessary, given the new threats that we now face and the unique nature of the threats facing the nation's capital.

U.S. national security should be of the utmost importance as WMATA considers bids for its procurement of 8000-series rail cars, and we therefore request that you consider submitting an addendum to the earlier RFP to ensure that the necessary steps are taken to protect against the aforementioned concerns.

We appreciate your prompt attention to this matter.

Sincerely,



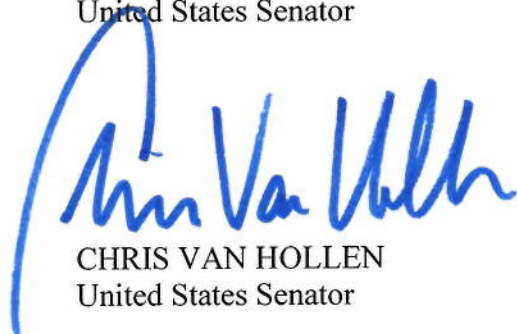
MARK R. WARNER
United States Senator



BENJAMIN L. CARDIN
United States Senator



TIM KAINE
United States Senator



CHRIS VAN HOLLEN
United States Senator